REMARKS

Upon entry of the present Amendment, claims 1-22 are pending in the application. New claims 20-22 are added. No new matter is presented.

Claims 1-5 and 17 stand rejected under 35 U.S.C. § 112, second paragraph, claim 18 is rejected under 35 U.S.C. § 101 as allegedly being directed to non-statutory subject matter, claims 1-4, 6-9, 11-14 and 16-19 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Krishnan et al. (U.S. Patent No. 6,405,316, hereinafter "Krishnan"), and claims 5, 10 and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Krishnan in view of Lotspiech et al. (U.S. Patent No. 6,118,873, hereinafter "Lotspiech"). The outstanding rejections are addressed below.

Claim Rejections - 35 U.S.C. § 112, second paragraph

As best understood, the Examiner alleges that the limitations of "means for performing a first decryption" and "means for performing a second decryption", as defined by claim 1 are indefinite because "since no function is specified by the word(s) preceding 'means', it is impossible to determine the equivalents of the element." In support of this rejection, the Examiner relies on *Ex parte Klumb*. Applicant respectfully disagrees.

Initially, the word "means" is not preceded by "for performing", rather "for performing" clearly follows means. Moreover, the Examiner's reliance on *Ex parte Klumb* is misplaced. In *Ex parte Klumb*, the claim limitations at issue were "plate means" and "wing means" which were recited without specifying any function to be performed. In other words, "means", as recited in the claim, was merely preceded by "plate" or "wing". *Ex parte Klumb* 159 USPQ 694, 694-695 (Bd. App. 1967). Thus, *Ex parte Klumb* held that a "structureless term without a function specified therefore affords no basis for judging whether a structure different from that disclosed by applicant would be an equivalent thereof." *Klumb* at 695 (emphasis added).

However, in stark contrast to the "plate means" and "wing means" in Klumb, claim 1 clearly defines the function performed by the means. For instance, claim 1 recites, *inter alia*, "means for performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key" and "means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key". In both instances, a specified function is recited. *See* MPEP § 2181.

Further, the Examiner's contention that the equivalents of the recited elements are "impossible" to determine is inconsistent with the clear support found in the specification. In this regard, the Examiner is kindly referred to Figure 1 and the corresponding description in the specification, which discloses both means for performing a first decryption and means for performing a second decryption, as recited.

Applicant notes that the above comments are equally applicable to claim 17, which stands rejected on similar grounds. In view of the foregoing, the rejection of claims 1-5 and 17 under 35

U.S.C. § 112, second paragraph is improper, and reconsideration and withdrawal of the rejection is requested.

Claim Rejections - 35 U.S.C. § 101

The Examiner asserts that claim 18 is directed to a system for decrypting an encrypted computer program that is "functional descriptive material" that does not fall within the statutory classes listed in 35 U.S.C. § 101. Applicant traverses this ground of rejection.

Initially, Applicant notes that the Examiner "bears the initial burden...of presenting a prima facie case of unpatentability." *See* In re Oetiker, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). As demonstrated below, Applicant respectfully disagrees that the Examiner has established that the subject matter of claim 18 is non-statutory.

In this regard, Applicant notes that claim 18 defines a **method** for decrypting an encrypted computer program, comprising, *inter alia*, performing a decryption of a plurality of blocks, wherein for each of said plurality of blocks, a cipher key is generated from a current block and a next block is decrypted with the cipher key. Thus, claim 18 defines a process, which is clearly within the statutory classes listed in 35 U.S.C. § 101.

Further, Applicant additionally submits that claim 18 recites statutory subject matter *at least* because the method defined by claim 18 provides a physical transformation of the plurality of blocks of the computer program. As recited, a cipher key is *generated* from a current block and a next block is *decrypted* with the cipher key.

Moreover, the Examiner has not demonstrated that the subject matter of claim 18 does not otherwise produce a useful, concrete, and tangible result. Rather, the Examiner incorrectly identifies claim 18 as being directed to a system, and the assertion that the claim recites only "functional descriptive material" is inconsistent with the physical transformation noted above.

Therefore, reconsideration and withdrawal of the rejection of claim 18 is requested.

Claim Rejections - 35 U.S.C. § 102

As noted above, claims 1-4, 6-9, 11-14 and 16-19 are rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by Krishnan.[1] This ground of rejection is traversed.

Independent claims 1, 6, and 11 respectively define a novel system, method, and computer program product for decrypting an encrypted computer program. For instance, claim 6 recites a method comprising, *inter alia*, generating a first cipher key from at least one first block of the encrypted computer program; performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; and performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key.

Notwithstanding the Examiner's rejection, Applicant submits that Krishnan fails to teach or suggest all the limitations of claim 6. For example, Krishnan clearly fails to teach a "first decryption" and "second decryption" as claimed. Rather, Krishnan merely teaches an incremental decryption routine for decrypting injected dynamic link library (DLL) or security code stored within an executable file that "decrypts each block of data previously encrypted and executes each block, one at a time, so that the entire code is never decrypted and executed at once." *See* Krishnan at col. 12, lines 13-16 and col. 16, lines 29-33. As shown in Figure 14, the incremental decryption routine merely performs a single loop over all of the encrypted blocks beginning with the first block, and each block is decrypted key determined from designated CPU flags. *See* Krishnan at col. 16, lines 39-47. When the last block is decrypted, the decryption routine ends. *See* Krishnan at col. 17, lines 6-14. Thus, Krishnan, at most, teaches a <u>single encryption process</u> where each of the blocks of the security code are sequentially decrypted based on the state of CPU flags. See Krishnan at col. 16, lines 51-61.

Conversely, claim 6 clearly requires <u>both</u> a first decryption and a second decryption. As recited, a first cipher key is generated from at least one first block of the encrypted computer program. Subsequently, a first decryption is performed <u>on a plurality of second blocks</u> of the encrypted computer program with the first cipher key. Next, a second decryption is performed

[1] Applicant notes that page 4 of the Office Action apparently incorrectly states that claims 1-4, 6-9 11-14 and 16 are the claims rejected under 35 U.S.C. § 102(e) based on Krishnan, while the Examiner additionally relies on Krishnan in the rejection of claims 17-19 on pages 8-9.

on the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. Thus, the "plurality of second blocks" are first decrypted by the first cipher key and the same plurality of second blocks are subsequently decrypted in sequence individually, in which a second cipher key is generated for each of the plurality of second blocks from a current block to decrypt the next block of the second plurality of blocks. Thus, the method defined by claim 6 provides for two layers of decryption.

Krishnan, however, merely teaches a single layer of "incremental decryption" of blocks. Indeed, the Examiner contends that col. 13, lines 45-47 and col. 16, lines 40-47 teach the feature of "performing a first decryption of a plurality of second blocks". See Office Action at page 5. However, col. 13, lines 45-47 merely teaches that the corresponding encryption routine of Krishnan sets up each encrypted block to "ensure that each block can be decrypted and executed independently from every other block." Likewise, col. 16, lines 40-47 merely teaches that the incremental decryption routine "begins as loop over all of the encrypted blocks beginning with the first block" in which a current block is decrypted with a determined key.

Thus, the Examiner is improperly relying on the incremental decryption loop of Krishnan to teach both the first decryption and the second decryption. This "incremental decryption" cannot correspond to both the "first decryption" and "second decryption", as claimed. Krishnan does not suggest that a plurality of blocks are decrypted with a first cipher key generated from at least one first block and the same plurality of blocks are then individually decrypted according to the claimed second decryption.

In addition, Applicant disagrees that the Examiner's assertion that the subject matter of a "second cipher key is generated from a current block and a next block is decrypted with the second cipher" is disclosed at col. 16, lines 57-63 and col. 17, lines 3-6 of Krishnan. For instance, steps 1404 and 1410 (see Fig. 14 of Krishnan) are merely provided in order to send the CPU flag state obtained when just completing steps 1403 to steps 1401 and 1402, which will be executed for the next data block. Further, step 1405 to 1409 are inserted between step completed step 1403 and step 1411. In other words, the set of steps defined by steps 1404 to 1410 are merely a type of use of a stack memory. The CPU flag state saved at step 1404 is restored at step 1410 and eventually set as "a key" at step 1402 executed the next time. "The key" set at step 1402 is used for decrypting a current data block at step 1403 executed next time. However, the CPU flag state changes many times during the execution of step 1403, and the CPU flag state at the end of executing step 1403 is saved at step 1404 and eventually used for decrypting the next data block.

Thus, according to Krishnan, a key for decrypting a certain block is obtained from a flag state of a CPU which has executed another block. By contrast, as defined by claim 6, a key for decrypting a certain block is generated from another block itself. Krishnan, however, does not teach at least the feature of performing a second decryption of the plurality of second blocks, wherein for each of the plurality of second blocks, a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. Rather, as noted above, Krishnan teaches that a key for decrypting a block is obtained from a flag state of a CPU.

In view of the foregoing, the rejection of claim 6 is improper because Krishnan fails to teach or suggest all the recited limitations. Therefore, reconsideration and withdrawal of the rejection of claim 6 is requested. Further, the above arguments are equally applicable to claims 1 and 11, which recite similar features and are believed to be allowable for the same reasons. In addition, dependent claims 2-5, 7-10 and 12-15 and 20-22 are believed to be allowable at least by virtue of depending from claims 1, 6, and 11 respectively.

Claim 16

Independent claim 16 defines a computer readable medium which recites the features of the plurality of encrypted blocks are encrypted with a cipher key generated from said non-encrypted block, and for each of the plurality of encrypted blocks, a next block is encrypted with a cipher key which is generated from a current block. As discussed above, Krishnan merely teaches a single layer of encryption of each of the blocks, and therefore cannot properly be relied upon to teach at least the above recited features. Thus, claim 16 is believed to allowable for similar reasons as discussed above with respect to independent claims 1, 6, and 11. Accordingly, reconsideration and withdrawal of the rejection is requested.

Claims 17-19

Independent claim 18 defines a method for decrypting an encrypted computer program comprising, *inter alia*, performing a decryption of a plurality of blocks, wherein for each of said plurality of blocks, a cipher key is generated from a current block and a next block is decrypted with said cipher key.

As discussed above with respect to claim 6, Krishnan teaches that a key for decrypting a certain block is obtained from <u>a flag state</u> of a CPU which has executed another block. By contrast claim 18 requires a key for decrypting a certain block is generated from <u>another block itself</u>. Thus, Krishnan fails to teach at least the feature of performing a decryption of a plurality of blocks, wherein for each of said plurality of blocks, a cipher key is generated from a current block and a next block is decrypted with said cipher key. Rather, as noted above, Krishnan teaches that a key for decrypting a block is obtained from a flag state of a CPU.

Accordingly, claim 18 is believed to be allowable and reconsideration and withdrawal of the rejection is requested. Further, Applicant submits that claims 17 and 19, which define a system and computer program product, respectively, reciting similar features as recited by claim 18 are allowable at least for the reasons discussed above with respect to claim 18. Therefore, allowance of claims 17 and 19 is requested.

Claim Rejections - 35 U.S.C. § 103

As noted above, claims 5, 10 and 15 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Krishnan in view of Lotspiech. Without commenting substantively on the grounds of rejection, Applicant submits that claims 5, 10 and 15 are allowable at least by virtue of depending from claims 1, 6, and 11, respectively.

New Claims

In order to provide additional coverage merited by the scope of the invention, Applicant is adding new claims 20-22. These claims are believed to be allowable at least by virtue of depending from claims 1, 6 and 11, respectively.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

Brian K. Shelton
Registration No. 50,245

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: November 28, 2005